Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
46346

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
10/786,405	February 26, 2004

First Named Inventor
Moon-Heui Lee et al.

Art Unit	Examiner
2139	Christian A. Laforgia

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record. Registration number 46,300

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

Signature

Christian C. Michel
Typed or printed name

(202) 659-9076
Telephone number

August 7, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 3 forms are submitted.

PATENT
Case Docket No.: 46346

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	:	
Moon-Heui Lee et al.	:	Group Art Unit: 2139
Serial No.: 10/786,405	:	Examiner: Christian A. Laforgia
Filed: February 26, 2004	:	Confirmation No.: 4007
For: METHOD FOR LOCKING AND RELEASING A CAMERA IN A PORTABLE TERMINAL	:	

ARGUMENTS FOR CONSIDERATION FILED CONCURRENTLY WITH PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This communication is submitted in response to the final office action of April 8, 2008. Applicants respectfully petition for a one month extension of time, fee included, and request consideration of the following:

Remarks/Arguments:

In the final Office Action mailed 04/08/2008, the Examiner rejects claims 8-11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Publication No. 2002/0106202 to Hunter in view of U.S. Patent Publication No. 2003/0008662 to Stern et al. ("Stern"), in further view of U.S. Patent No. 7,079,656 to Menzel et al. ("Menzel"). Applicants respectfully traverse these rejections.

In the Advisory Action of July 17, 2008, the Examiner states that one cannot show nonobviousness by attacking references individually were rejections are based on combinations

of references. Applicants submit, however, that it is proper to attack each applied reference individually if the Examiner has misinterpreted its teaching or lack thereof.

Hunter merely discloses portable cameras that receive signals from transmitters that cause one or more functions of the camera to be controlled accordingly. In response to receipt of the transmitted signal, the camera may be arranged to disable one or more functions of the camera. The camera is arranged to be enabled or active in a limited area or number of locations. *See* paragraph [0013]. Hunter further discloses a unit 100 housed within a portable camera and includes a smart card reader 102 for receiving a smart card 104 and a disable module 106 arranged to disable one or more of the functions of the portable camera, in accordance with data stored on the smart card 104.

However, there is nothing in Hunter that teaches a cipher apparatus that receives information of the portable terminal, obtains a secret code for the locked state of the camera from a database, and transmits enciphered data obtained from the secret code. Hunter does not teach that the portable camera receives and deciphers enciphered data and compares a secret code received from a cipher apparatus with one of the secret codes stored in the memory of the camera, nor that the camera is enabled when a secret code matches one of the secret codes stored in the memory. The data on the smart card of Hunter does not comprise a secret code.

The Examiner acknowledges that Hunter does not teach enciphering the data, receiving information of the portable terminal, and obtaining a secret code for the locked state of the camera from a database and alleges that Stern teaches a method for receiving information regarding the mobile user device and finding a policy based on the device and location information in a database which is sent to the mobile devices by referencing Figure 3, blocks 304 and 306, Figure 4, blocks 800 and 900, paragraphs [0053]-[0056], [0058] and [0059].

Stern further discloses a mobile user device 400 that operates in accordance with a location policy and user device information. *See* Abstract. The location policy refers to a rule or other type of information referring to the operation of a mobile user device within proximity to a location device. A location device 1000 may evaluate user device information and transmit an appropriate location policy to a mobile user device 400. Also, the location device 1000 may simply determine whether or not a location policy will be applied based on the user device information. *See* paragraphs [0052]-[0059].

However, there is nothing in Stern that teaches a cipher apparatus that receives information of the portable terminal, obtains a secret code for the locked state of the camera from a database, and transmits enciphered data obtained from the secret code. Nowhere does Stern teach that the portable terminal receives and deciphers enciphered data. Stern discloses a location device 1000 that receives user device information from a PDA indicating that the PDA is registered to a student. The location device 1000 compares the registration information of the PDA with the location policy and transmits information to the PDA indicating that the PDA is not allowed to wirelessly exchange information. *See* paragraph [0058].

Stern further discloses that the location device 1000 may also instruct a digital camera that no pictures are to be taken during a concert performance. The digital camera may then transmit an offer to provide payment of five dollars in exchange for permission to take ten pictures. The location device 1000 can then reject the offer, accepts the offer, or propose a counter-offer to the digital camera. *See* paragraph [0059]. The location device 1000 operates in accordance with a policy associated with a pre-defined set of rules for operation. *See* paragraph [0056]. Essentially, the mobile user device of Stern receives information from a location device 1000 comprising a location identifier (e.g., a concert hall or a school) and a location policy associated with the location (that is, a set of rules or other type of information that can be associated with the operations of the mobile user device.

However, there is nothing in Stern that teaches that the location device is a cipher apparatus that receives information of the mobile user device, obtains a secret code for the locked state of a camera from a database, and transmits enciphered data obtained from the secret code. Moreover, there is nothing in Stern that teaches that the mobile user device 400 of Stern receives and deciphers enciphered data. The mobile user device of Stern receives a location policy from a location device. Nowhere does Stern teach comparing a secret code received from the cipher apparatus with one of the secret codes stored in the memory, nor that a camera is enabled to operate when a secret code matches said one of the secret codes stored in the memory.

To cure the deficiencies of Hunter and Stern, the Examiner relies on Menzel for teaching a mobile device and a base station that exchange public keys, which the Examiner alleges as reading on the secret code of the present application, by referencing col. 2, lines 7-19 and col. 2, lines 48-58. The Examiner further alleges that Menzel teaches a method of encrypting data using the exchanged public keys in subsequent communication, citing col. 2, lines 9-19 and 51-58.

Menzel discloses a method for encrypting information for a radio transmission and for authentication of subscribers in a communication system. *See* col. 1, lines 9-12. The method of encryption of Menzel comprises encrypting subsequent information to be transmitted via the radio interface using one of the public keys received by the base station or the mobile station, and deciphering encrypted information received by the mobile station or the base station on the basis of a private key that is allocated to the transmitted public key in the mobile station or in the base station. *See* col. 2, lines 4-19. Menzel further discloses that the public keys received by the base station or mobile station is employed for the encryption of information to be subsequently transmitted via the radio interface, and the encrypted information received by the mobile station or the base station can be deciphered on the basis of a private key that is allocated in the mobile station or in the base station that the public key was transmitted.

According to the Examiner, it would have been obvious to one of ordinary skill in the art at the time the invention was made for a mobile device and a base station to exchange public keys and encrypt the data using the exchanged public keys in subsequent communication, since Menzel states at col. 3, lines 3-29 that encrypted communication provides for secure communication between the devices, thereby preventing unauthorized users from intervening in the exchange of information. However, Menzel does not teach that the public key transmitted by the mobile station to the base station and the public key employed by the base station comprise a secret code for the locked state of a camera from a database, nor that the private keys employed by the mobile station or base station are obtained from a secret code for the locked state of a camera from a database.

Information of Menzel is encrypted for radio transmission. *See* col. 2, lines 20-22. Transmitters in the mobile station and base station mutually send public keys via a radio interface. Controllers in the mobile station and the base station encrypt the information sent via the radio interface upon employment of public keys received by the base station or the mobile station. Accordingly, public keys and private keys are mutually sent to each other. However, the base station or mobile station of Menzel does not transmit public keys that correspond to a secret code for a locked state of a camera. Furthermore, the private keys of Menzel do not comprise enciphered data obtained from a secret code. Nowhere does Menzel teach comparing a secret code received from a cipher apparatus with one of the secret codes stored in a memory and

enabling a camera to operate when the secret code matches said one of the secret codes stored in memory.

Menzel discloses a mobile station that sends a first public key via a radio interface in parallel for all subscribers active at it and makes note of an appertaining private key that is deposited in the memory or the controller. The base station employs the received public key for the encryption of information to be subsequently sent via the radio interface. The deciphering of the information sent by the base station is thus only possible for the entity that knows the appertaining private key, i.e., the mobile station with the private key. The base station in turn sends a public key in reply of the base station and makes note of the appertaining private key. The memory or the controller of the base station stores the private key. Information subsequently sent by the mobile station to the base station, which is encrypted upon employment of the public key, can only in turn be deciphered by the base station or its controller. Menzel does not teach comparing a public key with a public key stored in the memory, enabling a camera to operate when the public key matches one of the public keys stored in memory, nor that enciphered data is transmitted to a portable terminal and subsequently, the portable terminal deciphers the enciphered data. The public keys and private keys of Menzel are mutually sent between the base station and mobile station. Accordingly, Menzel does not disclose a method for comparing a secret code received from the cipher apparatus with one of the secret codes stored in the memory and enabling a camera to operate when the secret code matches said one of the secret codes stored in memory.

Accordingly, neither Hunter, Stern nor Menzel, alone or in combination, discloses, teaches or suggests the features of claims 8-11 and Applicants, therefore, request withdrawal of the rejection.

In view of the above, it is believed that there is at least one or more errors or omissions in the Examiner's rejections.

Respectfully submitted,

Christian C. Michel
Attorney for Applicants
Reg. No. 46,300

Dated: August 7, 2008